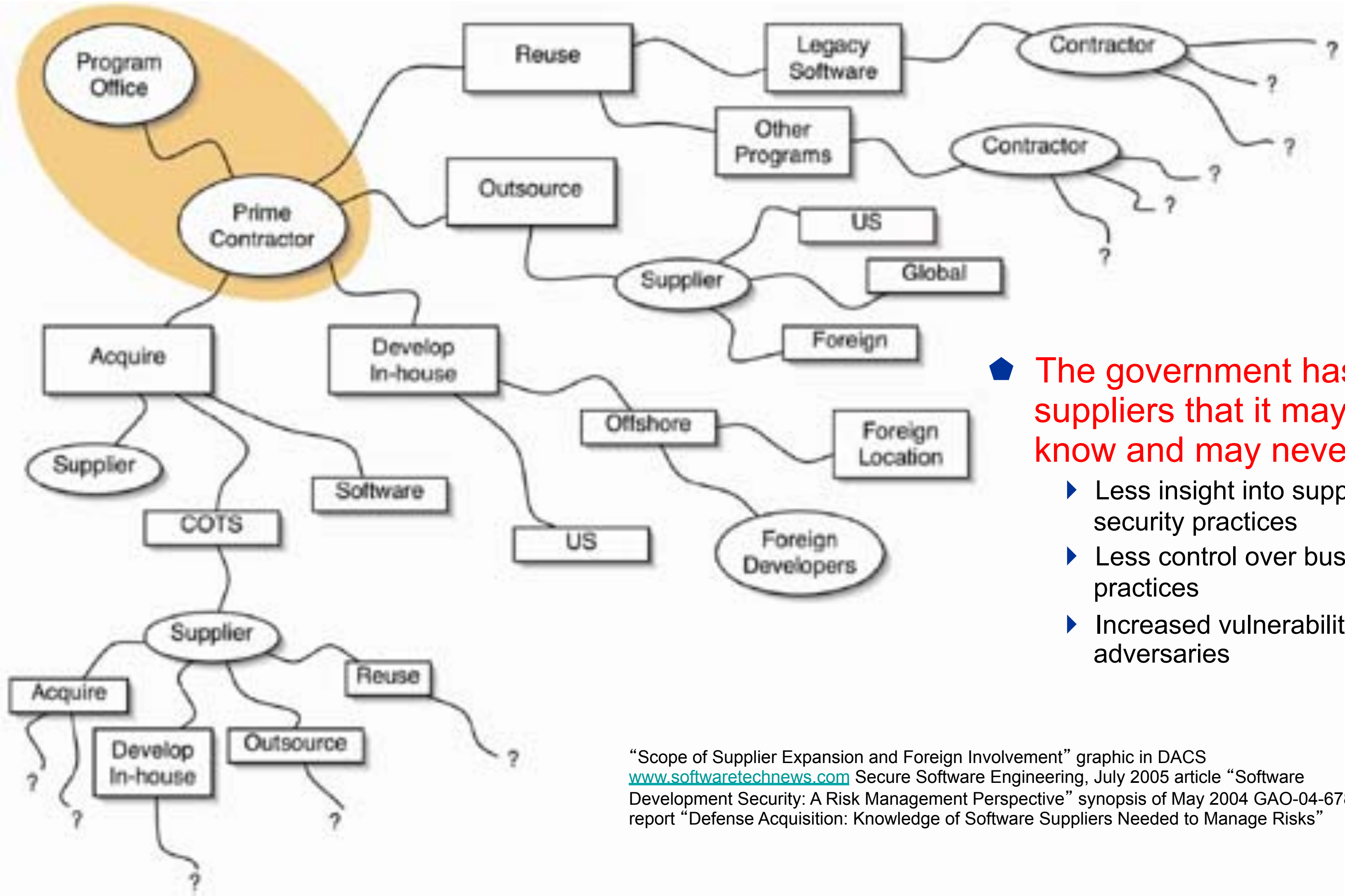
Globalization is good, but it brings challenges



- <span style="color:red">The government has suppliers that it may not know and may never see</span>
  - Less insight into suppliers' security practices
  - Less control over business practices
  - Increased vulnerability to adversaries

"Scope of Supplier Expansion and Foreign Involvement" graphic in DACS www.softwaretechnews.com Secure Software Engineering, July 2005 article "Software Development Security: A Risk Management Perspective" synopsis of May 2004 GAO-04-678 report "Defense Acquisition: Knowledge of Software Suppliers Needed to Manage Risks"

ICT components enable our Digital / Information Age

- Dependencies on technology are greater then ever

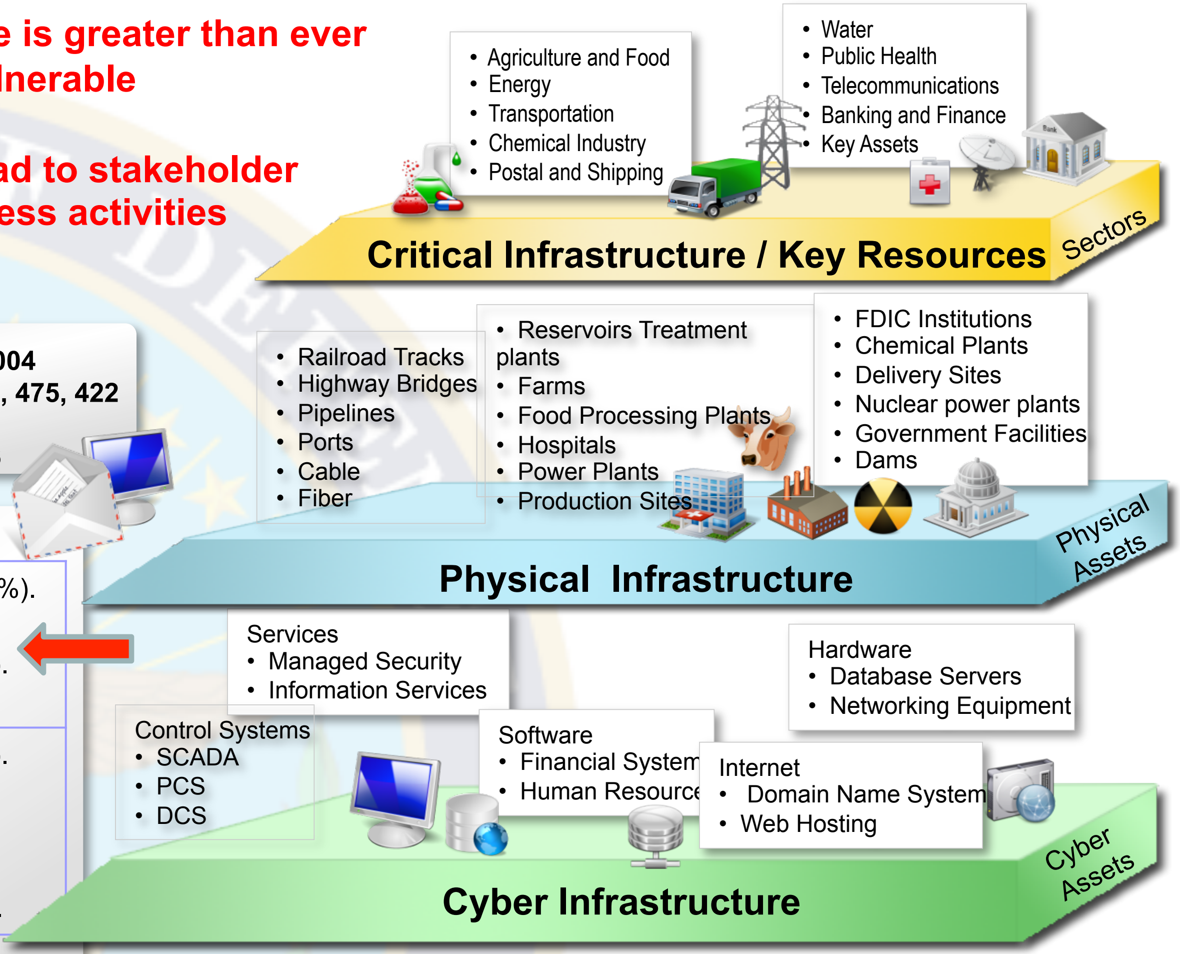
-- Possibility of disruption/sabotage is greater than ever because hardware/software is vulnerable

--- Loss of confidence alone can lead to stakeholder actions that disrupt critical business activities

Internet users in the world: 1,766,727,004
E-mail messages sent today: 215, 674, 475, 422
Blog Posts Today: 458, 972
Google searches Today: 2,302,204,936

Who is behind data breaches?	**74%** resulted from external sources (+1%). **20%** were caused by insiders (+2%). **32%** implicated business partners (-7%). **39%** involved multiple parties (+9%).
How do breaches occur?	**7%** were aided by significant errors (<>). **64%** resulted from hacking (+5%). **38%** utilized malware (+7%. **22%** involved privilege misuse (+7%). **9%** occurred via physical attacks (+7%).

** Source – 2009 Verizon Data Breach Investigations Report*



Critical Infrastructure / Key Resources — Sectors

- Agriculture and Food
- Energy
- Transportation
- Chemical Industry
- Postal and Shipping

- Water
- Public Health
- Telecommunications
- Banking and Finance
- Key Assets

Physical Infrastructure — Physical Assets

- Railroad Tracks
- Highway Bridges
- Pipelines
- Ports
- Cable
- Fiber

- Reservoirs Treatment plants
- Farms
- Food Processing Plants
- Hospitals
- Power Plants
- Production Sites

- FDIC Institutions
- Chemical Plants
- Delivery Sites
- Nuclear power plants
- Government Facilities
- Dams

Cyber Infrastructure — Cyber Assets

Services
- Managed Security
- Information Services

Hardware
- Database Servers
- Networking Equipment

Control Systems
- SCADA
- PCS
- DCS

Software
- Financial System
- Human Resource

Internet
- Domain Name System
- Web Hosting

Not only do we have an

increasingly

Global-Interdependent Supply Chain,

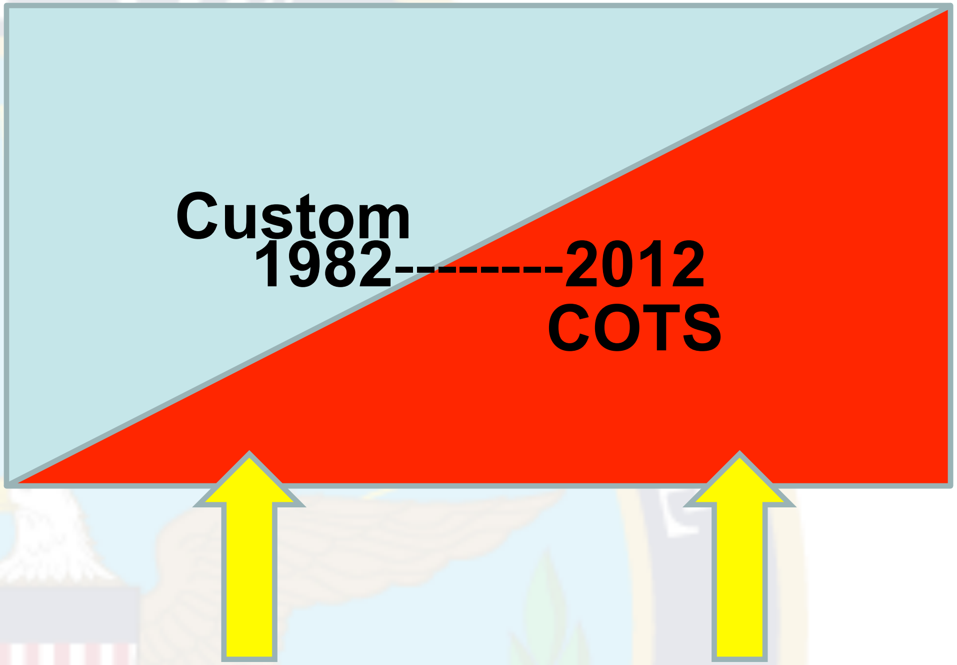
we also have a world of

Capabilities, that are

increasingly

Dependent on Globally Sourced ICT.

…also…increasingly Dependent on COTS products



Govt-SCRM-related Developments

- CNCI-SCRM still alive & well

- CNSS DIRECTIVE 505 on SCRM from Committee on National Security Systems (FOUO)

- NIST-IR 7622 & NIST 800-53 rev4 due soon (US.gov-only participates in SCRM WG2)

http://csrc.nist.gov/news_events/index.html

NIST hosted Public-Private SCRM Workshop on 15-16 Oct2012

- "IT Supply Chain: National Security-Related Agencies Need to Better Address Risks", GAO-12-361, Mar 23

http://www.gao.gov/products/GAO-12-361

both DOE & DOJ have now "stood-up SCRM Focal Points"

- DODI 5200.mm on Trusted Systems & Networks…VERY NEAR PUBLICATION
- USD AT&L Memo on Program Protection Planning (PPP) July 2011
- Monthly TSN RoundTable Meetings & NEW Quarterly TSN/PP Executive Council Meetings

Recent Evolution of Strategy & Policy

Counterfeit Microelectronics---L&MR lead

Who is working this (DoD, US,gov, public-private, standards)
& NDAA’12 Section 818…upcoming NDAA’13 ?

-Learn from Quality Assurance & Safety Critical Items Practices
-Procurement & Acquisition-Contracts
-Testing (life cycle doc, acceptance, follow-up analysis)
-Reporting
-WorkForce Development (training & education)
-Standards

Software Assurance---AT&L-SE lead

Who is working this (DoD, US,gov, public-private, standards)
& NDAA’11 Section 932… upcoming NDAA’13 ?

-Learn from Quality Assurance & Safety Critical Items Practices
-Procurement & Acquisition-Contracts
-Testing (life cycle doc, acceptance, follow-up analysis)
-Reporting
-WorkForce Development (training & education)
-Standards

HW/SW-Test SOAR Update

- **Mini-SOAR / SOAR-lite effort** deemed success w/o final report- (draft to be issued)- purpose was leader visibility & establish need for HW/SW-testing SOAR in FY13.

- **FY13 SOAR PURPOSE**: Provide state-of-the-art software, hardware, and integration information for Program Offices via "SOAR"-like product addressing security aspects for HW/SW components (with emphasis on acceptance testing &/or required test-documentation)… read as risk mitigation tools for incorporation in PPP.

Current Testing-SOAR Activity

- **SOAR on Security T&E of HW/SW**
  - ATL&CIO **baseline Testing SOAR** product initiated now with FY12$
    - —Product by October 2013
    - —Published in hardcopy via DTIC? by December 2013
    - —**Develop "document" in anticipation of being web-enabled**
  - ATL&CIO & NSA-CAS fund(s) updated for SOAR+ follow-on with FY13$
    - —Demonstrate product as **web-enabled digital media** capable of regular update and refresh with on-demand hard copy production
    - —Add annex/appendix on current DoD concerns; such as **mobility HW/SW security**, integrated T&E security extensions
    - —**Continue development of emerging immature content**; such as Integrity Test and Analyses (ITA) for sophisticated adversaries exploiting Supply Chain and other opportunities (including classified annex)
- **Vehicle to Execute**
  - FY12$ Contract-Task with IDA
  - FY13$- TBD